Disaster Recovery Response Plan

RFP 45732-4609 **APPENDIX B-1**

Article I. Roles, Responsibilities, Agreements

Section 1.01 Support Contracts and Agreements

Organization	Start Date	End/Renewal Date	Location / Sites	Escalation Contact Name	Escalation Contact Phone / Email
IBM	1/1/2023	12/31/2024	AWS Us East / West		
RedHat	1/1/2023	12/31/2024	AWS Us East / West		
Fortigate	1/1/2023	12/31/2024	AWS Us East / West		
AWS	1/1/2023	12/31/2024	AWS Us East / West		AWS Console

Section 1.02 Support Key Contacts

Location / Sites	Name	Phone (list primary first)	Email (list primary first)	Role(s)	Availability (Day / Hours)	State / Vendor
Maine - Augusta				Div Director, Program Policy & Performance	24/7	ReEmployME
Maine - Augusta				Cyber Security Manager	24/7	ReEmployME
Maine - Augusta				Deputy Director		ReEmployME
Maine - Augusta				Director		ReEmployME
Maine - Augusta				Deputy Commissioner		ReEmployME
Maine - Augusta				Commissioner		ReEmployME
Cary,NC 27513				Senior programmer Analyst		ReEmployME
MS – Jackson				Business Relationship Manager	24/7	ReEmployUSA / TCS

MS – Jackson				Technical Architect	24/7	ReEmployUSA / TCS
MS – Jackson				Infrastructure Lead	24/7	ReEmployUSA / TCS
MS – Jackson				Support Lead	24/7	ReEmployME / TCS
MS – Jackson				Suppport Lead	24/7	ReEmployMS / TCS
CT - Central Office				Decision maker	24/7/365	ReEmployCT
CT - Central Office				Decision maker	24/7/365	ReEmployCT
CT - Central Office Annex				Support	Normal Business Hours	ReEmployCT
CT - Central Office				Support	Normal Business Hours	ReEmployCT
CT - Central Office				Tester	Normal Business Hours	ReEmployCT
CT - Central Office				Decision maker	24/7/365	ReEmployCT
CT - Central Office				IT	24/7/365	ReEmployCT
CT - Central Office				IT	24/7/365	ReEmployCT
MDES State Office				CIO, OTSI Security Manager, OTSI	Business hours/After hours when needed	ReEmplyMS
MDES State Office				Network Manager, OTSI Security Manager, OTSI	Business hours/After hours when needed	ReEmplyMS

Section 1.03 Support Roles(s) / Responsibilities

ID	Name	Components Supported	Organization	Responsibilities
TC101	Infrastructure Lead	Operations and Coordination	TCS	Troubleshoot, Affect Repair Verify DR environment
TC102	OS (Linux) Admin	Operating System	TCS	Address any OS level issues Perform any OS level changes
TC103	DB2 Admin	DB Server	TCS	Perform steps for HADR

ID	Name	Components Supported	Organization	Responsibilities
TC104	Network Security Admin	IPS Edge Gateway	TCS	Changes to IPS system or Elastic IP's
TC105	Build Manager	Build Deployment-UrbanCode Deploy	TCS	Perform application level changes, start & stop various server components
TC106	Support Manager	Batch Scheduling Coordination	TCS	Ensure proper flow and functionality of systems Perform application verification
TC108	On-Call Batch Monitor	Biz and Batch Server	TCS	Monitor Application performance
ST101	Network Admin	State IPS system State VPN tunnel	State	Update DNS for IP address changes Support in case of any issues to the VPN tunnel or state firewall
ST102	Fortiweb Admin	Fortiweb appliance	TCS	Publish/Remove Maintenance page on Fortiweb
ST103	Vormetric Admin	Vormetric appliance	State	No work would be needed on the appliance during the DR. The admin needs to be available in case of any issues with Vormetric
ST104	Guardium Admin	Guardium appliance	State	No work would be needed on the appliance during the DR. The admin needs to be available in case of any issues with Guardium
ST105	DB2 Admin	DB2 Server	State	Perform DB2 HADR steps
ST106	Manager	Application Verification	State	Ensure application verification is performed successfully
ST107	Executive Director	DR Approval	State	Provide Approval for DR site to be live
CE101	AWS Elastic DRS Support Engineer	AWS Elastic DRS Console	TCS	Perform Failover and Failback
AWS101	AWS Support Engineer	AWS Cloud Console	TCS	Manage AWS Instances

Article II. Infrastructure

Section 2.01 Component / Configuration Documentation Inventory

ID	Component / Configuration	Location / Site	Confirming Role(s)	Repository / Location
	MS Application Server 1		TC105 & CE101	
	MS Application Server 2		TC105 & CE101	
	MS Application Server 3		TC105 & CE101	
	MS Application Server 4		TC105 & CE101	
	MS Application Server 5		TC105 & CE101	
	MS Biz and Batch Server		TC105,TC108 & CE101	
	MS DB2 Server		ST105	
	MS DB2 HADR Server		ST105	
	MS HornetQ and Workflow Server		TC105 & CE101	
	MS JSCape Server		TC105 & CE101	
	MS Identity Management Server		TC101 & CE101	
	MS Passive DMS Server		TC105 & CE101	
	MS RedHat Directory Server		TC102	
	MS RedHat Directory Server – Replica		TC102	
	COMMON Occucoder server		TC105 & CE101	
	COMMON Elastic Search DMS		TC105	
	COMMON Elastic Search DMS		TC105	
	COMMON Elastic Search DMS		TC105	
	MS IBM Worklight Server		TC105 & CE101	
	MS Log Server		TC102 & CE101	
	MS Fortinet IPS		TC104	
	MS Vormetric		ST103	
	MS Secondary Vormetric		ST103	
	MS Fortiweb		ST102	
	MS Guardium		ST104	
	ME Application Server 1		TC105 & CE101	
	ME Application Server 2		TC105 & CE101	
	ME Biz and Batch Server		TC105,TC108 & CE101	
	ME DB2 Server		ST105	
	ME DB2 HADR server		ST105	

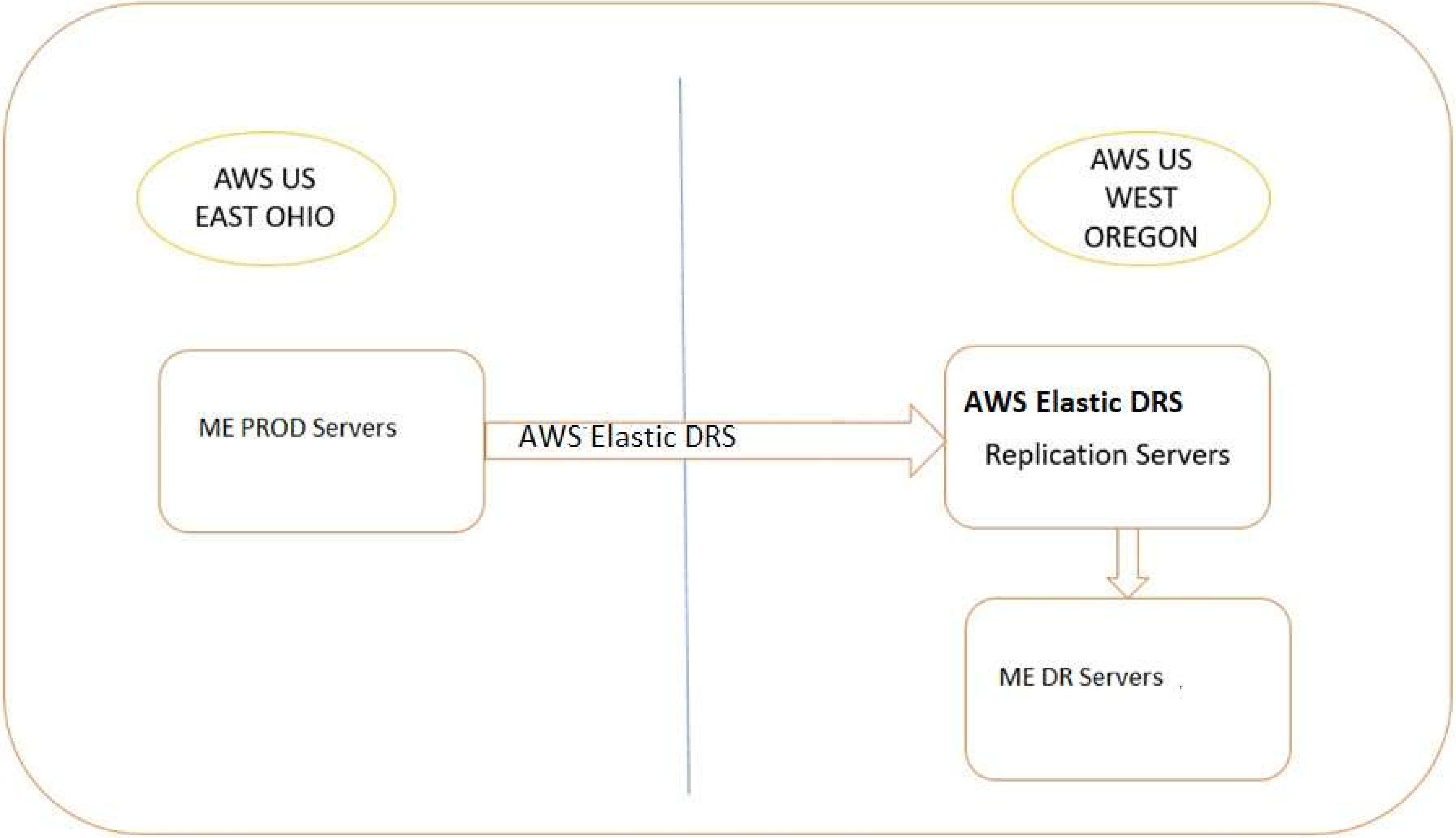
ID	Component / Configuration	Location / Site	Confirming Role(s)	Repository / Location
	ME HornetQ and Workflow Server		TC105 & CE101	
	ME JSCape Server		TC105 & CE101	
	ME Identity Management Server		TC101 & CE101	
	ME Log Server		TC102 & CE101	
	ME RedHat Directory Server		TC102	
	ME RedHat Directory Server – Replica		TC102	
	ME Fortinet IPS		TC104	
	ME Vormetric		ST103	
	ME Secondary Vormetric		ST103	
	ME Foriweb		ST102	
	ME Guardium		ST104	
	CT Fortinet IPS		TC104	
	CT Foriweb		ST102	
	CT Guardium		ST104	
	CT Vormetric		ST103	
	CT Application Server 1		TC105 & CE101	
	CT Application Server 2		TC105 & CE101	
	CT Application Server 3		TC105 & CE101	
	CT Application Server 4		TC105 & CE101	
	CT Application Server 5		TC105 & CE101	
	CT Application Server 6		TC105 & CE101	
	CT Application Server 7		TC105 & CE101	
	CT Application Server 8		TC105 & CE101	
	CT Application Server 9		TC105 & CE101	
CTUIMAPP0010	CT Application Server 10		TC105 & CE101	
	CT Application Server 11		TC105 & CE101	
	CT Biz and Batch Server		TC105,TC108 & CE101	
	CT DB2 Server		ST105	
	CT HornetQ and Workflow Server		TC105 & CE101	
	CT JSCape Server		TC105 & CE101	
	CT Identity Management Server		TC101 & CE101	
	CT Log Server		TC102 & CE101	
	CT RedHat Directory Server		TC102	
	CT RedHat Directory Server		TC102	

ID	Component / Configuration	Location / Site	Confirming Role(s)	Repository / Location
	CT RedHat Directory Server – Replica		TC102	
	CT Vormetric DR		ST103	
	CT DB2 HADR server		ST105	
	CT Fortinet IPS DR		TC104	
	CT Foriweb DR		ST102	
	AWS Cloud Console		AWS101	

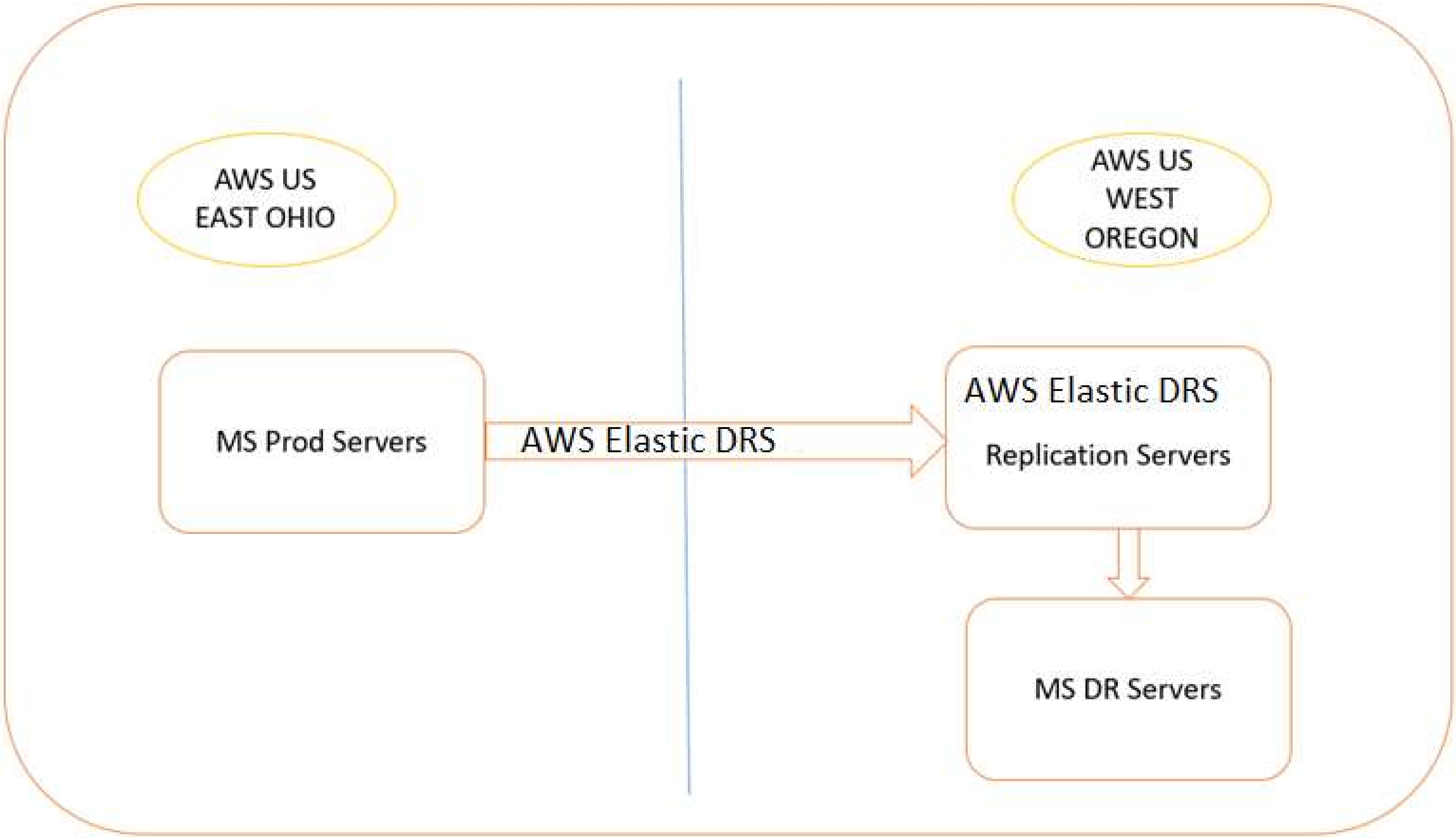
Note: Each component whose outage impact performance of the solution must be identified and included on relevant diagrams. This includes servers, appliances, virtual machines, peripherals, communication devices, network resources, etc. Each confirming role must be identified as secondary verification of event.

Section 2.02 Hardware / Architectural Diagram(s):

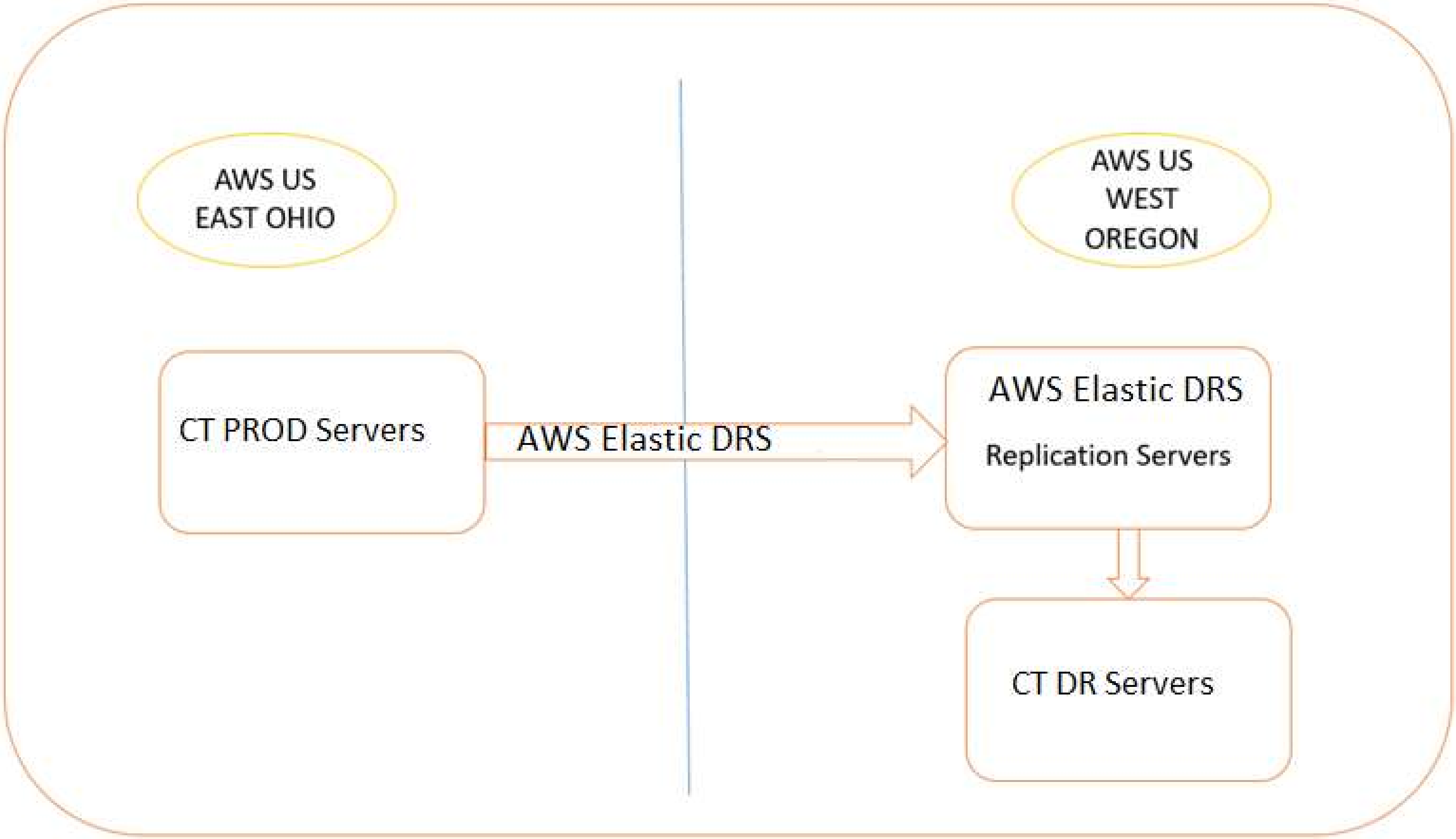
(a) ME US East-US West AWS sites



(b) MS AWS US EAST – US WEST

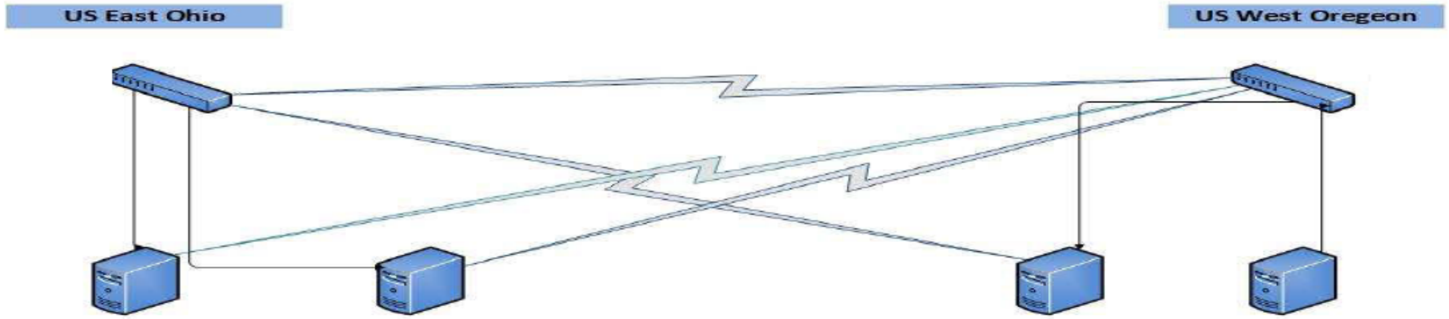


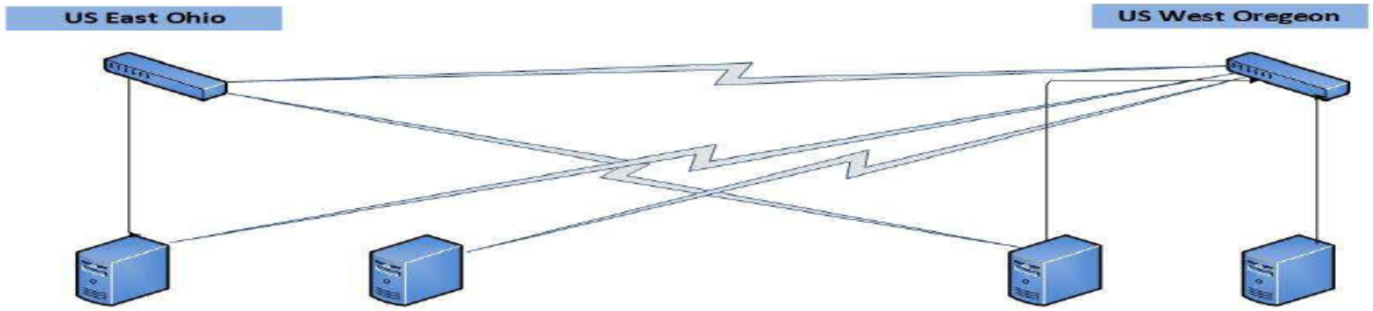
(c) CT AWS US EAST – US WEST

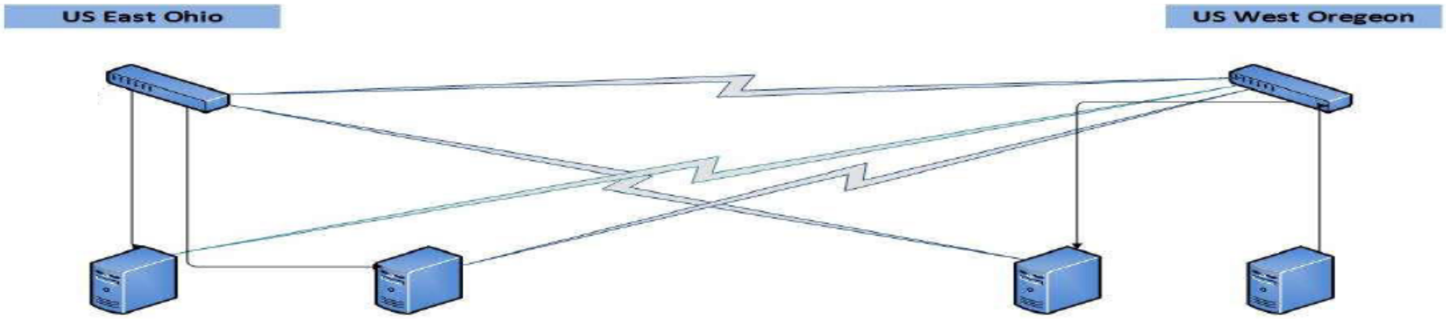


Section 2.03 Data / Communications Diagram(s):

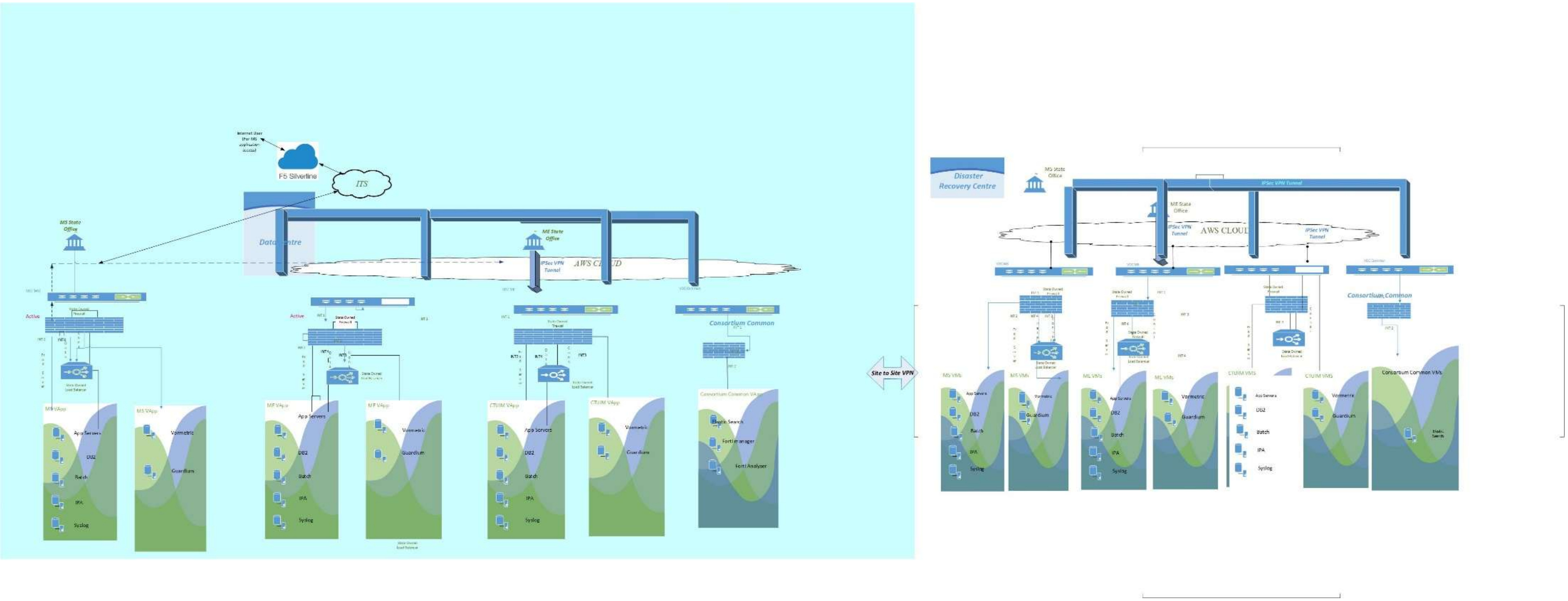
(a) Vormetric Appliance communication Ohio-Oregon AWS sites


US East Ohio
US West Oregeon


US East Ohio
US West Oregeon


US East Ohio
US West Oregeon

(b) Network Architecture Diagram Ohio-Oregon AWS sites



Section 2.04 Location / Site Variance Reference:

Location / Site (Primary)	Location / Site (Secondary)	Comp / Cfg ID	Remediation

External IP Address (Elasti IP's) assigned to Fortigate.	External IP Address (Elasti IP's) assigned to Fortigate.	AWS101	External IP addresses will be different for the 2 sites and DNS would need to be updated during DR for these changes. <Refer to the document table with the difference in the IP addresses>. This is only applicable for Maine.
Load Balancer	Fortiweb	ST102	
Clumio Backup Solution	NA	NA	Backup will be stored only in the Primary site. For the duration of CR, backups will not be available.

Section 2.05 Infrastructure Support Documentation Inventory

ID	Summary Description	Location / Site	Repository / Location
DR101	Disaster Recovery Test Execution Plan Document		
DR102	DR Response SW Install Documentation		
ISD101	Installation: RH linux ver. 7		
ISD102	Installation: RH linux ver. 8		
ISD103	Installation: RH directory server ver. 11		
ISD104	Installation: IBM Installation Manager ver. 1.8.3		
ISD105	Installation: WAS ND (Liberty) ver. 9		
ISD106	Installation: DB2 ver. 11.1.3.3		
ISD107	Installation: Jscape ver. 8.8		
ISD108	Installation: DMS/Jackrabit ver. X		
ISD109	Installation: DSM ver. X		
ISD110	Installation: Occucoder ver. 17		
ISD111	Installation: Spectrum Address validation ver. 11		
ISD112	Installation: Mailstream Plus ver. 8.03.03		
ISD113	Installation: Drools ver. 5.1		
ISD114	Installation: TDM ver. 11.3		
ISD115	Installation: Quartz ver. X		
ISD116	Installation: JAVA ver. 8		
ISD117	Installation: Mobile first ver. 8		
ISD118	Installation: Birt server ver. 4.2		

ID	Summary Description	Location / Site	Repository / Location
ISD119	Installation: IBM Cognos ver. 11.0.6		
ISD120	Installation: Guardium server ver. 11		
ISD121	Installation: Optium Archive ver. 11.3		
ISD122	Installation: Clumio Backup		
ISD123	Installation: Connect direct ver. 4.6		
ISD124	Installation: Vormetric Data Security Manager ver. 6.3.0.13038		
ISD125	Installation: Vormetric Transparent Encryption ver. 6.3.0.13038		
ISD126	Installation: Fortigate ver. 7.0.0		
ISD127	Installation: Deep Security for Linux		

Article III. Failover Response Measures

Section 3.01 RPO / RTO Level Definitions

(a) AWS Ohio

Comp / Cfg ID	RPO (Actual HH:MM:SS.mmm)	RPO (Target HH:MM:SS.mmm)	RTO (Actual HH:MM:SS.mmm)	RTO (Target HH:MM:SS.mmm)	Dependencies *(CID = Component ID)*
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		NA		NA	Preconfigured in DR
		NA		NA	Cluster with MSDRVOR01
		NA		NA	Preconfigured in DR
		NA		NA	Preconfigured in DR
		00:15:00.000		24:00:00.000	
MESOAPP02		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	

Comp / Cfg ID	RPO (Actual HH:MM:SS.mmm)	RPO (Target HH:MM:SS.mmm)	RTO (Actual HH:MM:SS.mmm)	RTO (Target HH:MM:SS.mmm)	Dependencies *(CID = Component ID)*
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		NA		NA	Preconfigured in DR
		NA		NA	Cluster with MEDRVOR01
		NA		NA	Preconfigured in DR
		NA		NA	Preconfigured in DR
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	
		NA		NA	Preconfigured in DR
		NA		NA	Preconfigured in DR
		NA		NA	Preconfigured in DR
		NA		NA	Preconfigured in DR
		00:15:00.000		24:00:00.000	
		00:15:00.000		24:00:00.000	Cluster with Elastic DR
		00:15:00.000		24:00:00.000	Cluster with Elastic DR

Note: Replace time based definitions with transaction/record definitions where appropriate. If both applicable, include additional record.

Section 3.02 Service Level Response Levels

(a) Vendor / Contract Controls

(b) Internal Controls

Article IV. Failover Event Definitions

Note: Events are identified by an outage of components or configured functionality where the RPO is exceeded. Responses are determined by the category assigned to the event. Categories are determined based on the list of components / configurations which can result in an event.

Section 4.01 Category 1: 100% Impact

MS Comp / Cfg ID	ME Comp / Cfg ID	CT Comp / Cfg ID	Additional Information / Exceptions
<ALL>	<ALL>	<ALL>	Entire AWS environment for a state(s) is down
			If the IPS server in primary is down for more than XX hours.

Section 4.02 Category 2: Partial Location / Site Specific Impact

(a) AWS US EAST OHIO – Database down

MS Comp / Cfg ID	ME Comp / Cfg ID	CT Comp / Cfg ID	Additional Information / Exceptions
			DB server down for more than XX hours

(b) AWS US EAST OHIO – Application down

MS Comp / Cfg ID	ME Comp / Cfg ID	CT Comp / Cfg ID	Additional Information / Exceptions
			Clustered with other application servers
			Clustered with other application servers
			Clustered with other application servers
			Clustered with other application servers
			Clustered with other application servers
			Clustered with other application servers
			If all application instances are down for more than XX hours.
			If Load Balancer instances in primary are down in primary for more than XX hours.

(c) AWS US EAST OHIO – LDAP down

MS Comp / Cfg ID	ME Comp / Cfg ID	CT Comp / Cfg ID	Additional Information / Exceptions
			RHDS instances in primary is down in primary for more than XX hours.
			Clustered with CTUIMRHDS002
			Clustered with CTUIMRHDS001

			RHDS instances in primary is down in primary for more than XX hours.

(d) MS AWS US EAST OHIO – Vormetric down

MS Comp / Cfg ID	ME Comp / Cfg ID	CT Comp / Cfg ID	Additional Information / Exceptions
			Servers will point to the secondary DSM in the DR site.

Section 4.03 Category 3: External Partner Impact

In event of environment failure on the External Data partner for key interfaces, Following are the components that can trigger external Partner Impact

Comp / Cfg ID	Additional Information / Exceptions
	In case of ICON application down for more than XX hours. Data exchange related to Interstate and federal inquiries will be down for that duration.
	In case of SIDES application down for more than XX hours. Employer/TPA SIDES Push and Pull will be down for that duration

Section 4.04 Category 4: Internal Partner Impact

Comp / Cfg ID	Additional Information / Exceptions
	WINGS is down for more than XX hours. Non-critical business components will not work during the duration: Job details for claimant based on preference, Sending Claimant signup and enrollment information to ES system.

Section 4.05 Category 5: Archival Impact

(a) Permanent/Long-term Outage

If the impact is permanent, then a new backup solution would need to be procured and deployed. Until the new solution is in place, backup operation of the identified server will have to be performed manually.

Section 4.06 Category 6: Controlled Event

Comp / Cfg ID	Additional Information / Exceptions
<ALL>	Entire AWS environment for a state(s) are planned to be brought down in view of an controlled event e.g. a predicted natural disaster

Article V. Failover Communication / Notification Procedures

Note: All communications must utilize standardized communication formats located within the sample/template repository to prevent non-confirming communications distribution impacting timeliness of communication/notification receipt.

Section 5.01 Category 1: 100% Impact

Time (Seq)	Format	Origin	Response (Y/N)	Confirm (Y/N)	Sample/Template Repository
E + 00:00:05:00	Email	Automated (AMS Support)	N	Y	
	Notes				

Note: One time/format per communication / notification line item. Response = Expected Response Confirm = Confirmation of Receipt Required

Section 5.02 Category 2: Partial Location / Site Specific Impact

(a) Location / Site [X]

(b) Location / Site [X]

Section 5.03 Category 3: External Partner Impact

Section 5.04 Category 4: Internal Partner Impact

Section 5.05 Category 5: Archival Impact

Section 5.06 Category 6: Controlled Event

Article VI. Failover Operational Procedures / Recovery Processes Checklists

Section 6.01 Category 1: 100% Impact

MS Comp / Cfg ID	ME Comp / Cfg ID	CT Comp / Cfg ID	Additional Information / Exceptions	Procedure
<ALL>	<ALL>	<ALL>	Entire AWS environment for a state(s) is down	Execute the DR Failover Steps as defined in Section 3 of Disaster Recovery Test Execution Plan Document.
			If IPS server in primary is down for more than XX hours.	Execute the DR Failover Steps as defined in Section 3 of Disaster Recovery Test Execution Plan Document.

Section 6.02 Category 2: Partial Location / Site Specific Impact

(a) AWS Ohio vDC – Database down

MS Comp / Cfg ID	ME Comp / Cfg ID		Additional Information / Exceptions	Procedure
			DB server down for more than XX hours	Execute the DB2 HADR Failover Steps as defined in Section 5.1 of DR101 - Disaster Recovery Test Execution Plan Document.

(b) AWS Ohio vDC – Application down

MS Comp / Cfg ID	ME Comp / Cfg ID		Additional Information / Exceptions	Procedure
			Clustered with MESOAPP002 and MESOAPP003	Since the servers are running in clustered environment, if one server fails then the traffic will be routed to other server(s). Team will analyze and rectify the issue and make sure that the affected server becomes operational as quickly as possible.
			Clustered with MESOAPP001 and MESOAPP003	Since the servers are running in clustered environment, if one server fails then the traffic will be routed to other server(s). Team will analyze and rectify the issue and make sure that the affected server becomes operational as quickly as possible.

MS Comp / Cfg ID	ME Comp / Cfg ID		Additional Information / Exceptions	Procedure
			Clustered with other app servers	Since the servers are running in clustered environment, if one server fails then the traffic will be routed to other server(s). Team will analyze and rectify the issue and make sure that the affected server becomes operational as quickly as possible.
			Clustered with other app servers	Since the servers are running in clustered environment, if one server fails then the traffic will be routed to other server(s). Team will analyze and rectify the issue and make sure that the affected server becomes operational as quickly as possible.
			Clustered with other app servers	Since the servers are running in clustered environment, if one server fails then the traffic will be routed to other server(s). Team will analyze and rectify the issue and make sure that the affected server becomes operational as quickly as possible.
			Clustered with other app servers	Since the servers are running in clustered environment, if one server fails then the traffic will be routed to other server(s). Team will analyze and rectify the issue and make sure that the affected server becomes operational as quickly as possible.
			Clustered with other app servers	Since the servers are running in clustered environment, if one server fails then the traffic will be routed to other server(s). Team will analyze and rectify the issue and make sure that the affected server becomes operational as quickly as possible.
			Clustered with other app servers	Since the servers are running in clustered environment, if one server fails then the traffic will be routed to other server(s). Team will analyze and rectify the issue and make sure that the affected server becomes operational as quickly as possible.
			If all application instances are down for more than XX hours.	Execute section 5.9, Switch to DR App Servers For DR of DR101 - Disaster Recovery Test Execution Plan Document.
			If Fortiweb instance in primary is down in primary for more than XX hours.	Execute Section 5.8, Switch Fortiweb Servers, of DR101 - Disaster Recovery Test Execution Plan Document.

(c) AWS Ohio vDC – LDAP down

MS Comp / Cfg ID	ME Comp / Cfg ID	CT Comp / Cfg ID	Additional Information / Exceptions	Procedure
			If all the RHDS instance in primary is down in primary for more than XX hours.	We will start the LDAP servers on the DR site and reconfigure the App Servers and Workflow server to use the DR Site LDAP as defined in Section 5.7, LDAP IP Change on App Server and Workflow Server of DR101 - Disaster Recovery Test Execution Plan Document.
			Clustered with CTUIMRHDS002	Since the servers are running in clustered environment, if one server fails then the traffic will be routed to other server(s). Team will analyze and rectify the issue and make sure that the affected server becomes operational as quickly as possible.
			Clustered with CTUIMRHDS001	Since the servers are running in clustered environment, if one server fails then the traffic will be routed to other server(s). Team will analyze and rectify the issue and make sure that the affected server becomes operational as quickly as possible.
			If all the RHDS instance in primary is down in primary for more than XX hours.	We will start the LDAP servers on the DR site and reconfigure the App Servers and Workflow server to use the DR Site LDAP as defined in Section 5.7, LDAP IP Change on App Server and Workflow Server of DR101 - Disaster Recovery Test Execution Plan Document.

(d) AWS Ohio - Vormertic down

Comp / Cfg ID			Additional Information / Exceptions	Procedure
MS Comp / Cfg ID	ME Comp / Cfg ID	CT Comp / Cfg ID	Servers will point to the secondary DSM in the DR site.	Servers will point to the secondary DSM in the DR site.

Section 6.03 Category 3: External Partner Impact

Comp / Cfg ID	Additional Information / Exceptions
	Communicate with ICON for an alternate site in case the primary site is down.

	Communicate with SIDES for an alternate site in case the primary site is down.

Section 6.04 Category 5: Archival Impact

(a) Manual Backup

Following tables lists down the critical components and the Backup frequency that needs to be performed manually

MS Comp / Cfg ID	ME Comp / Cfg ID	CT Comp / Cfg ID	Manual Backup Frequency	Additional Information / Exceptions
			Daily	
			Daily	
			Daily	
			Daily	
			Daily	
			Daily	
			Daily	
			Daily	Store last 3 Backups
			Daily	
			Daily	
			Daily	
			Daily	
			Daily	
			Daily	
			Daily	
			Daily	
			Daily	
			Daily	
			Daily	
			Daily	
Elasticdr			Daily	
HQSOGRP002			Daily	

Section 6.05 Category 6: Controlled Event

Comp / Cfg ID	Additional Information / Exceptions	Procedure
<ALL>	Entire AWS environment for a state(s) is down	Execute the DR Failover Steps as defined in Section 3 of Disaster Recovery Test Execution Plan Document.

Article VII. Fallback Criteria Definitions

States need to provide their criteria for determining when to fallback (Sync Times, Push times or verification).

Article VIII. Fallback Communication / Notification Procedures

Note: All communications must utilize standardized communication formats located within the sample/template repository to prevent non-confirming communications distribution impacting timeliness of communication/notification receipt.

Section 8.01 Location / Site [X]

Time (Seq)	Format	Origin	Response (Y/N)	Confirm (Y/N)	Sample/Template Repository
E + 00:00:05:00	Email	Automated (AMS Support)	N	Y	DMS 00001: AMS Support Center Cleveland
	Notes				External Distribution List Repository
					HD987 - Help Desk WIKI

Note: One time/format per communication / notification line item. Response = Expected Response Confirm = Confirmation of Receipt Required

Section 8.02 Location / Site [X]

Article IX. Fallback Operational Procedures / Recovery Processes Checklists

Section 9.01 AWS US East Ohio

Following table lists down the checklist of items that needs to be verified in order to determine the environment to be ready for fallback:

Category	MS Comp / Cfg ID	ME Comp / Cfg ID		Checklist
Networking				1. Connectivity from On-premise to Cloud over VPN 2. Connectivity from MS ITS to Cloud over internet 3. Connectivity from Cloud to internet 4. Connectivity between the VM's will have to be verified after the restore from DR site
VM				1. Each of the VM is UP and accessible 2. OS networking - Host entry and resolv.conf entries are correct. On each VM This will have to be verified after the restore from DR site
AWS				1. Connectivity and traffic coming into AWS gateway to MS Fortigate and then on to the VMs
Common				1. Each of the Fallback steps identified in the Section 4 of Disaster Recovery Test Execution Plan Document have been executed.

Article X. Event Monitoring

This section would need to be elaborated further once we have the detailed solution for the Monitoring tool which is Elastic APM

Section 10.01 AWS US EAST Ohio

(a) Console / Monitoring Tools

Console / Tool	Scope
Elastic APM	Server Ping URL Monitoring Email Notification

(b) Verification / Monitoring Scripts

Console / Tool	Alert Type	Remarks
Elastic APM	Following for all servers: CPU Memory File System utilization Disk utilization	

(c) Event Log Repository Inventory

Console / Tool	Location
Elastic APM	Even logs will be maintained and accessible within the tool